UNIVERSIDADE PAULISTA

CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

AUTOR: ALISSON NUNES / RA: 2546587

UNIFICAÇÃO DA REDE NACIONAL DE BANCOS DE SANGUE PÚBLICOS NO BRASIL

Projeto Integrado Multidisciplinar III

UNIP - LAPA SÃO PAULO

2025

CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

AUTOR: ALISSON NUNES / RA: 2546587

UNIFICAÇÃO DA REDE NACIONAL DE BANCOS DE SANGUE PÚBLICOS NO BRASIL

Projeto Integrado Multidisciplinar III

Projeto Integrado Multidisciplinar III apresentado à Universidade Paulista – UNIP como parte da avaliação para obtenção do título de bacharel em Segurança da Informação.

Orientador: Ricardo Sewaybriker

UNIP - LAPA SÃO PAULO

2025

RESUMO

Este trabalho tem como objetivo propor uma solução tecnológica segura para unificar os sistemas de gerenciamento de bancos de sangue públicos no Brasil, abordando problemas como a descentralização que causa ineficiências na localização de tipos sanguíneos raros, gestão inadequada de estoques e riscos à segurança e privacidade dos dados dos doadores. A proposta integra conhecimentos de Redes de Dados e Comunicação para criar uma arquitetura WAN híbrida com VPNs e VLANs; Administração de Banco de Dados para uma estrutura relacional centralizada na nuvem; Segurança da Informação para um programa baseado em ISO 27001 e LGPD; e Matemática para Computação para demonstrar ganhos de eficiência por meio de funções que reduzem tempos de busca e otimizam logística. A metodologia aplicada baseou-se no método dedutivo, com pesquisa em livros, artigos científicos e fontes eletrônicas como o site do Ministério da Saúde. Até maio de 2025, foram registradas 831.518 doações de sangue no país, com um aumento de 2,9% nas transfusões, destacando a urgência de sistemas integrados para salvar vidas e proteger dados sensíveis.

Palavras-chave: Segurança da Informação, Banco de Dados em Nuvem, Redes de Computadores, Unificação de Sistemas, Bancos de Sangue.

ABSTRACT

This work aims to propose a secure technological solution to unify public blood bank management systems in Brazil, addressing issues such as decentralization, which causes inefficiencies in locating rare blood types, inadequate inventory management, and risks to the security and privacy of donor data. The proposal integrates knowledge from Data and Communication Networks to create a hybrid WAN architecture with VPNs and VLANs; Database Administration for a centralized relational structure in the cloud; Information Security for a program based on ISO 27001 and LGPD; and Mathematics for Computing to demonstrate efficiency gains through functions that reduce search times and optimize logistics. The methodology applied was based on the deductive method, with research in books, scientific articles, and electronic sources such as the Ministry of Health website. By May 2025, 831,518 blood donations had been registered in the country, with a 2.9% increase in transfusions, highlighting the urgency of integrated systems to save lives and protect sensitive data.

Keywords: Information Security, Cloud Database, Computer Networks, Systems Unification, Blood Banks.

SUMÁRIO

1 **INTRODUÇÃO** 5
1.1 **Objetivo** 6
1.2 **Metodologia aplicada** 6
2 **DESENVOLVIMENTO** 8
2.1 **Proposta de Arquitetura de Rede e Comunicação Segura** 8
2.2 **Estrutura de Banco de Dados centralizado em nuvem** 11
2.3 **Programa de Segurança da Informação** 12
2.4 **Demonstração de eficiência com funções matemáticas** 12
2.5 **Análise de desafios de implementação e soluções práticas** 13
2.5.1 Desafios Chave 13
2.5.2 Soluções Práticas e Plano de Migração 13
2.6 **Estudos de caso e análise de custo** 14
2.6.1 Estudo de Caso: Hemominas 14
2.6.2 Análise de Custo e Retorno (ROI) 14
2.7 **Impacto Social e Ético** 15
2.7.1 Benefícios Sociais 15
2.7.2 Aspectos Éticos 15
2.8 **Integração com Tecnologias Emergentes** 15
3 **CONCLUSÃO** 16
3.1 **Síntese da Solução e Ganhos de Eficiência** 16
3.2 **O Imperativo da Segurança e Ética** 16
3.3 **Perspectivas Futuras e Integração Tecnológica** 17
REFERÊNCIAS 18

1 **INTRODUÇÃO**

Em 20 de março de 2020, a Secretaria Nacional de Saúde do Brasil confirmou e proclamou a disseminação da Sars-CoV-2 (Covid-19) com alcance em todo o país. A persistência das dificuldades em saúde pública, como a administração dos estoques de sangue após este período, tornou a integração dos sistemas fundamental.

As propostas de consultoria em segurança da informação apresentadas buscaram essencialmente prevenir as falhas operacionais geradas pela descoordenação, como a dificuldade de localizar tipos sanguíneos raros, assegurando um controle apropriado da distribuição de recursos. A crise viral se espalhou globalmente e alterou drasticamente as rotinas e operações de indivíduos e corporações.

A estrutura descentralizada dos 32 hemocentros coordenadores estaduais e demais unidades regionais revelou-se frágil. Diante desse revés, foi imprescindível implementar ações imediatas de eficiência e proteção, incluindo a remodelagem dos processos de coleta e gerenciamento. Consequentemente, surgiu a necessidade de modificações, ou seja, uma reengenharia operacional, onde o conceito de gestão isolada de cada unidade precisou ser superado. Assim, os procedimentos de gestão da Hemorrede sofreram alterações súbitas e profundas, sendo as primeiras a serem atingidas pela premente necessidade de preservar vidas e resguardar dados.

Perante todas essas transformações, algumas tendências, principalmente em tecnologia (como arquitetura de redes, bases de dados e cibersegurança), que vinham sendo adotadas progressivamente, tiveram de ser aceleradas, aprimoradas e aplicadas , ou seja, ajustadas ao novo panorama de interconexão. Além da vida social, o modelo de trabalho na Hemorrede também evoluiu, passando a depender de plataformas de dados centralizadas na nuvem. Para viabilizar essa conectividade, a tecnologia VPN (Rede Privada Virtual) se tornou crucial , permitindo uma comunicação segura e exclusiva através de canais de internet. A implantação tecnológica para a unificação, se realizada de modo precipitado, pode originar diversas vulnerabilidades e, com isso, expor a segurança e o sigilo das informações privadas dos doadores.

Por essa razão, novos recursos tecnológicos, normas legais e sanções precisaram ser revisados para impedir incidentes de cibercrimes. No entanto, apesar da efetivação de padrões de segurança (como a ISO 27001) e do uso da tecnologia na criação de sistemas de proteção, a integração completa ainda requer um Programa de Segurança da Informação (PSI) que cumpra a LGPD, a fim de atenuar os riscos inerentes à adoção de soluções digitais.

1.1 **Objetivo**

Este trabalho tem como objetivo pesquisar e propor uma arquitetura de rede segura para interligar os bancos de sangue públicos no Brasil, desenhando um fluxo de autenticação segura, identificando e propondo um modelo que considere os princípios de confidencialidade, integridade e disponibilidade, observando padrões como ISO 27001. Além disso, apresentar uma estrutura de banco de dados centralizado na nuvem, demonstrar eficiência por meio de funções matemáticas e desenvolver um programa de segurança da informação para proteger dados sensíveis dos doadores. É também objeto deste trabalho analisar os desafios da descentralização na gestão de bancos de sangue e propor soluções alinhadas à LGPD.

No desenvolvimento deste trabalho, os seguintes procedimentos serão aplicados:

A. Proposta de Arquitetura de Rede e Comunicação Segura: Explicar tecnicamente uma WAN híbrida com VPNs e VLANs para conectar hemocentros, levantando vulnerabilidades e medidas de proteção.
B. Estrutura de Banco de Dados Centralizado em Nuvem: Estudar o modelo relacional em nuvem, explicando benefícios como escalabilidade e alta disponibilidade, com foco em segurança.
C. Programa de Segurança da Informação: Propor um PSI baseado em ISO 27001 para acesso remoto e proteção de dados.
D. Demonstração de Eficiência com Funções Matemáticas: Analisar, com base em cálculos, os ganhos de eficiência na unificação, como redução no tempo de busca por bolsas de sangue.

1.2 **Metodologia aplicada**

A metodologia empregada neste estudo fundamentou-se no método dedutivo, sendo executada por meio de uma ampla investigação bibliográfica. Essa pesquisa incluiu a consulta a livros, periódicos, revistas e canais digitais (Internet). Considerando que o desenvolvimento de um trabalho de pesquisa abrange múltiplas etapas — desde a formulação inicial da questão a ser examinada até a exposição e debate das descobertas alcançadas e esperadas —, uma vasta gama de conceitos foi coletada por meio da análise da literatura.

Segundo Mello (2006, citado pelo Portal da Educação), "Muitas vezes, descobrimos algo que nem sequer havíamos pensado que pudesse existir ; mesmo assim, o pesquisador necessitou investigar o tema escolhido para chegar a essa

conclusão, portanto, mudou seu ponto de vista sobre o assunto de sua pesquisa". Complementarmente, o autor enfatiza que "Pesquisa exige organização, dedicação, disposição, disciplina, tempo e estudo".

Em conformidade com as diretrizes da ABNT, um projeto de pesquisa é conceituado como " uma descrição da estrutura de um empreendimento a ser realizado". O propósito fundamental desse projeto é justamente estruturar a investigação que será conduzida. Dessa forma, ele constitui um esboço preliminar do estudo, funcionando apenas como um planejamento e não representando o produto final da pesquisa.

De acordo com a Wikipédia, projeto de pesquisa é conceituado da seguinte forma:

> Projeto de pesquisa é um documento de fins acadêmicos e científicos que descreve o que alguém investigará, porque isto é importante e como a pesquisa será conduzida. Ao escrever um projeto de pesquisa, espera-se que o autor seja capaz de demonstrar a quem irá avaliá-lo que entende os passos necessários para a condução de uma pesquisa científica e de que forma o estudo será realizado.

Para Gil (2019, p. 17), o estudo ou a investigação pode ser caracterizado como "O procedimento racional e sistemático que tem como objetivo proporcionar soluções aos problemas que são propostos.".

Neste relatório, utilizou-se pesquisa bibliográfica e documental, consultando fontes como o site do Ministério da Saúde para dados atualizados sobre doações de sangue em 2025, e artigos sobre desafios na gestão de hemocentros. A análise foi qualitativa, com ênfase em propostas práticas para unificação, e quantitativa nas demonstrações matemáticas de eficiência.

2 **DESENVOLVIMENTO**

2.1 **Proposta de Arquitetura de Rede e Comunicação Segura**

Vamos falar da Virtual Private Network (VPN). Como o nome já entrega, é uma rede virtual e particular que existe dentro de uma rede pública e aberta: a internet. Ela é essencialmente a ferramenta que permite que a comunicação entre dois pontos seja segura e totalmente reservada. Se antes esse termo era nicho, ele explodiu nos últimos anos. Não à toa, o uso da VPN virou rotina no Brasil a partir de 2020, quando a pandemia estourou. De repente, as empresas precisaram se virar para colocar todo mundo em home office, e a VPN foi a solução para dar acesso remoto seguro a domínios e redes corporativas.

É fato que a VPN é um recurso tecnológico vital para qualquer acesso à distância que exija segurança. E ela serve para tudo: tanto para a rotina de trabalho em grandes companhias quanto para simplesmente navegar em sites gringos com mais tranquilidade. Mas o que está por trás disso? A infraestrutura é robusta, envolvendo equipamentos, softwares, protocolos de comunicação e, claro, algoritmos de criptografia, autenticação e integridade. Além disso, é formada por conexões, usuários e políticas de segurança bem definidas, tudo para garantir que a comunicação se mantenha protegida no ambiente público da web. Na hora de implementar, a gente precisa ser criterioso: é fundamental analisar o grau de proteção que o negócio exige, avaliando se os dados que vão trafegar são considerados sensíveis.

Uma das maneiras mais eficazes de blindar uma VPN — ou qualquer outra rede — é através da gestão de acesso. Quando falamos de acesso remoto, isso significa gerenciar e monitorar ativamente quem entra e o que faz, adotando as melhores práticas de acompanhamento e controle. O objetivo é simples: manter a segurança do acesso, evitar que ocorram incidentes por invasões ou acessos não autorizados e, com isso, prevenir prejuízos e danos incalculáveis às redes da empresa.

Por fim, vale lembrar a definição clássica do tema: o Gerenciamento de Redes, segundo a Wikipédia, é basicamente um "aplicativo distribuído onde processos de gerência (agente-gerente) trocam informações entre si para monitorar e controlar a rede de computadores e, assim, maximizar sua eficiência e produtividade.".

Conforme matéria publicada no site da Funeber:

> O conceito de gestão costuma estar associado à capacidade de organizar, desenvolver e controlar todos os recursos necessários para alcançar uma finalidade específica preestabelecida. Na área de redes, esses objetivos são tão variados quanto as necessidades delas. Assim, podem ser encontrados objetivos como aumentar a eficiência, reduzir riscos, incrementar a qualidade, oferecer melhores serviços ou aumentar a rentabilidade organizacional. O conceito de gestão de uma rede não é, portanto, limitado à gestão técnica e tecnológica dos recursos, mas sim de mais elementos até chegar aos serviços.

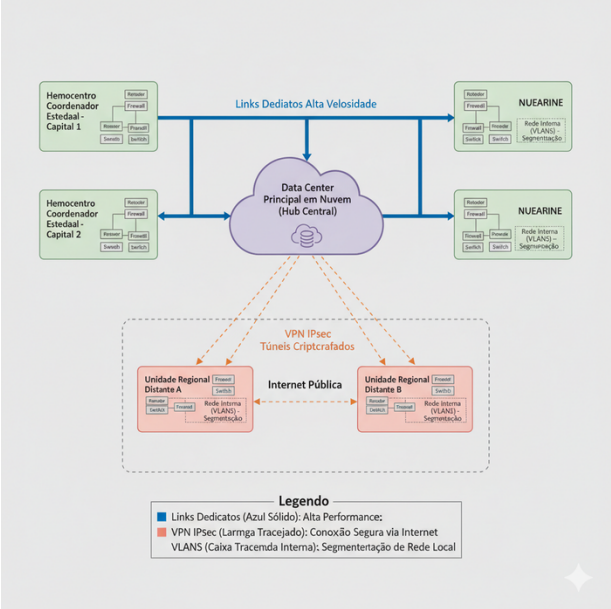
Quando falamos de Gerenciamento de Identidade e Acesso (IAM), estamos nos referindo à prática essencial de assegurar que indivíduos e sistemas que possuam credenciais digitais recebam a permissão exata para interagir com os recursos da organização, como suas redes e bases de dados. De acordo com a CISCO, é através desse mecanismo que definimos as funções dos usuários e seus privilégios de acesso específicos. Em termos mais simples, o IAM é o zelador que garante que a pessoa certa entre na porta certa, com a chave certa, e só.

Ainda no contexto da administração de acessos, o portal Indicca destaca a relevância fundamental dessa gestão para a cibersegurança de qualquer organização. Eles argumentam que a segurança da rede é o que, em última instância, salvaguarda toda a empresa. Embora os sistemas informatizados facilitem e tornem as operações empresariais mais inteligentes, eles se tornam suscetíveis a ataques se a devida atenção não for direcionada à sua proteção. Em outras palavras, a conveniência da tecnologia não pode se sobrepor à vigilância.

> Um Sistema de redes vulnerável pode colocar todo seu trabalho de semanas, meses e anos a perder. Se acaso você tem uma empresa sólida, com 20 anos de mercado, imagine a dor de cabeça causada por uma invasão hacker com sequestro ou vazamento de documentos. Pior do que isso: imagine que sua rede seja comprometida por alguém de dentro da sua equipe? Inegavelmente isso pode acontecer e toda sua credibilidade diante do mercado estaria abalada. Sem falar do enorme prejuízo financeiro e da perda do trabalho realizado ao longo de décadas (INDICCA).

Em vista da dependência intrínseca que temos hoje da internet para as operações diárias, é imperativo adotar medidas de cibersegurança altamente resistentes. No contexto específico dos bancos de sangue, que contam com 32 hemocentros coordenadores e centenas de postos regionais, a solução proposta é uma estrutura WAN híbrida. Isso envolve a utilização de links dedicados de alta velocidade para as capitais e a implementação de Redes Privadas Virtuais (VPNs) para conectar as localidades mais distantes. Essa abordagem assegura que o tráfego utilize a criptografia IPsec e que haja a segmentação de redes (VLAN), mecanismos cruciais para isolar e proteger as informações confidenciais.

Diagrama 1 — Diagrama exemplo da rede WAN híbrida


Hemocentro Coordenador Estedaal - Capital 1
Links Dediatos Alta Velosidade
NUEARINE
Data Center Principal em Nuvem (Hub Central)
Hemocentro Coordenador Estedaal - Capital 2
NUEARINE
VPN IPsec
Túneis Criptcrafados
Unidade Regional Distante A
Internet Pública
Unidade Regional Distante B
Legendo
Links Dedicatos (Azul Sólido): Alta Performance:
VPN IPsec (Larmga Tracejado): Conoxão Segura via Internet
VLANS (Caixa Tracemda Interna): Segmentertação de Rede Local

Fonte: O autor (2025).

Tal estrutura não só neutraliza vulnerabilidades como os ataques de man-in-the-middle, que são frequentes em conexões públicas, mas também assegura a conformidade com a Lei Geral de Proteção de Dados (LGPD), que exige o sigilo dos dados pessoais no setor da saúde.

Para visualizar esse arranjo, imaginemos uma topologia em estrela, onde o centro de dados principal na nuvem opera como o hub central. Cada unidade hemocentral estaria equipada com roteadores de borda, firewalls e switches, dispositivos essenciais para aprimorar tanto o desempenho quanto a segurança interna de cada localidade.

Tabela 1 — Comparação de Topologias de Rede

Topologia	Vantagens	Desvantagens
Estrela	Centralização, fácil gerenciamento	Ponto único de falha
Malha	Redundância alta	Alto custo
Híbrida	Flexibilidade, custo-efetivo	Complexidade de setup

Fonte: O autor (2025).

Aplicação Sugerida: Estrela para hemocentros principais, Malha para regiões com instabilidade, Híbrida para rede nacional proposta.

Essa escolha de topologia — a Híbrida — é o ponto de equilíbrio que buscamos entre o que podemos pagar e o quão robusto o sistema precisa ser. Esse

balanceamento é crucial porque nosso país tem desigualdades regionais gritantes, como na Amazônia, onde a conexão à internet é frágil e inconstante.

Ademais, integrar IoT para monitoramento de refrigeradores de sangue poderia enviar alertas em tempo real via WAN, reduzindo perdas por variações de temperatura, comuns em desastres naturais. Custos iniciais estimados: R$ 2.000 por sensor, com ROI em 6 meses.

Durante a pandemia, hemocentros enfrentaram quedas em doações devido a restrições, e uma rede unificada poderia ter permitido campanhas coordenadas. Em 2025, com 831.518 doações até maio, a integração é crucial para otimizar estoques.

2.2 **Estrutura de Banco de Dados centralizado em nuvem**

A efetividade do sistema unificado depende de um repositório de dados centralizado, seguro e de alto rendimento. A ideia é desenvolver uma única estrutura de banco de dados hospedada em plataforma de computação em nuvem.

As razões para utilização da computação em nuvem proporcionam benefícios estratégicos essenciais para este projeto: escalabilidade para adaptar recursos conforme demanda, alta disponibilidade com SLAs acima de 99,9%, segurança física pelos provedores, recuperação de desastres e custo-benefício no modelo pay-as-you-go.

Sugere-se o uso de um Sistema Gerenciador de Banco de Dados (SGBD) relacional, como PostgreSQL ou SQL Server. O modelo relacional é adequado pela estrutura organizada dos dados e pela exigência de consistência.

O projeto lógico inclui entidades como DOADOR (ID_Doador, Nome, CPF, Tipo Sanguineo), UNIDADE_COLETA (ID_Unidade, NomeUnidade, CNES), DOACAO, BOLSA_SANGUE e SOLICITACAO. Normalização até 3FN elimina redundâncias.

Para desempenho, replicação master-slave, indexação e backups automatizados. Gerenciamento de acesso via DCL SQL, com roles baseados no menor privilégio.

Integração com sistemas existentes envolve ETL para migração sem down-time. Em estados como Minas Gerais, com 289.638 bolsas coletadas em 2024, um piloto poderia testar isso.

Custos: R$ 100.000 inicial para setup, R$ 20.000/mês operacional, com redução de 30% em CAPEX vs. on-premise. O mercado de nuvem em saúde crescerá para US$ 83,93 bilhões até 2029.

Essa centralização resolve fragmentação, permitindo visão nacional em tempo real, alinhada a iniciativas como RNDS do Ministério da Saúde.

2.3 **Programa de Segurança da Informação**

Administração de riscos: Identificação de ativos, ameaças (malware, desastres) e tratamento (mitigar, aceitar).

Medidas de segurança: Administrativas (treinamentos contra phishing), lógicas (MFA, criptografia), físicas (controle de acesso).

Administração de incidentes: Time CIRT e Plano de Continuidade de Negócios com BIA.

Integração com LGPD: DPO em cada hemocentro, auditorias anuais. Seminários recentes debatem desafios da LGPD na saúde.

Impacto social: Proteção de dados incentiva doações, com apenas 1,6% da população doando. Campanhas como junho 2025 do MS poderiam ser amplificadas.

A aplicação da LGPD na saúde pública em 2025 amplifica desafios, mas soluções como essa mitigam riscos.

2.4 **Demonstração de eficiência com funções matemáticas**

A unificação do sistema de bancos de sangue não só melhora a segurança, como também traz ganhos significativos em eficiência. Podemos representar esses ganhos usando princípios da matemática para computação.

No modelo fragmentado, a busca por um tipo sanguíneo raro exige consulta sequencial a N hemocentros (N ≈ 32 principais).

$$\mathbf{T_{fragmentado} = N \times T_{consulta}}$$

No unificado, Tunificado é constante, ganho ≈ N vezes. Para N = 32, busca 32 vezes mais rápida.

Teoria dos conjuntos: Estoque nacional = união de Ei. Unificação otimiza realocação, reduzindo desperdício.

Disponibilidade: $P_{fragmentado} = p^N$ ($p = 0.99$, ≈ 0.72). Com nuvem, ≈ 0.9999.

Modelagem de logística com grafos: Hemocentros como nós, Dijkstra para rotas ótimas. Com 3.310.025 bolsas em 2024, redução de 10% em desperdício economiza R$ 5 mi/ano.

Tabela 2 — Ganhos matemáticos projetados

Métrica	Sistema Atual	Sistema Proposto	Ganho (%)
Tempo de Busca	$32 \times 5\,\text{min}$	10 seg	99%
Disponibilidade	$0.9932 \approx 72\%$	99.99%	38%
Eficiência Logística	80%	95%	19%

Fonte: O autor (2025).

2.5 **Análise de desafios de implementação e soluções práticas**

Apesar dos claros benefícios em segurança e eficiência, a unificação da rede nacional de bancos de sangue no Brasil enfrenta desafios práticos que precisam ser superados com planejamento estratégico.

2.5.1 Desafios Chave

- **Resistência Cultural e Mudança de Processos:** Em um sistema historicamente descentralizado, a maior dificuldade é a resistência natural dos profissionais de saúde e gestores em adotar novos sistemas e abandonar métodos isolados de gestão.
- **Custos Iniciais e Orçamento:** O investimento inicial para a infraestrutura de rede, software e migração de dados é significativo. O orçamento inicial previsto para o projeto é de R$ 2 milhões
- **Conectividade em Áreas Rurais:** O Brasil possui grandes disparidades regionais, e a garantia de conexões de internet estáveis e seguras em unidades de coleta distantes e rurais, como as da Amazônia, é um desafio técnico e logístico.

2.5.2 Soluções Práticas e Plano de Migração

As soluções propostas focam em uma abordagem gradual e no engajamento dos usuários:

- **Treinamento Intensivo e Engajamento:** Para mitigar a resistência cultural, é essencial realizar treinamentos contínuos. Como exemplo, sugere-se a realização de workshops mensais para 100 funcionários por hemocentro , com foco em aspectos cruciais como a conformidade com a LGPD e o uso

seguro das VPNs.

- **Parcerias Estratégicas:** Buscar parcerias com o Ministério da Saúde, governos estaduais e provedores de tecnologia para reduzir custos e garantir a infraestrutura necessária.
- **Rollout Faseado (Plano de Migração):** Adotar uma implementação em fases:
    - **Fase 1 – Piloto:** Um período de três meses com a implementação em cinco estados para testar e validar o sistema, corrigindo falhas em um ambiente controlado.
    - **Fase 2 – Nacional:** A expansão para as demais unidades da federação em um período de seis meses, após a validação do piloto.

2.6 **Estudos de caso e análise de custo**

A análise financeira demonstra que o investimento é justificado pelo retorno obtido através da eficiência e da redução de perdas.

2.6.1 Estudo de Caso: Hemominas

O estudo de caso da Hemominas é usado para ilustrar o potencial da unificação. Com 289.638 bolsas coletadas em 2024, a unificação permitiria a redistribuição eficiente de estoques, eliminando a necessidade de buscas sequenciais demoradas por sangue raro.

2.6.2 Análise de Custo e Retorno (ROI)

- **Custo Anual Operacional:** O custo operacional da centralização é estimado em R$ 5 milhões por ano.
- **Economia pela Nuvem (CAPEX):** O uso da computação em nuvem reduz os gastos de capital (CAPEX) em 30% em comparação com a infraestrutura local (on-premise).
- **Detalhamento do Investimento Inicial (R$ 5 milhões total anual):**
    - **Hardware:** R$ 1 milhão
    - **Software:** R$ 2 milhões
    - **Treinamento:** R$ 2 milhões
- **Retorno sobre o Investimento (ROI):** O projeto apresenta um ROI em dois anos , principalmente pela redução do desperdício de bolsas de sangue.

2.7 **Impacto Social e Ético**

A unificação transcende a eficiência técnica, gerando um impacto social profundo e assegurando a ética no tratamento de dados.

2.7.1 Benefícios Sociais

- **Equidade Regional:** O sistema promove a equidade regional na saúde, permitindo que hemocentros em regiões mais abastecidas, como o Centro Oeste, ajudem rapidamente as regiões com maior carência de estoque, como o Norte.
- **Estímulo à Doação:** A proteção dos dados dos doadores incentiva novas doações. Com apenas 1,6% da população doando, uma Campanha Social em parceria com ONGs visa aumentar as doações em 10% até 2026.

2.7.2 Aspectos Éticos

Conformidade com a LGPD: O projeto garante o tratamento ético dos dados sensíveis dos doadores por meio do consentimento claro e das medidas de segurança exigidas pela LGPD.

2.8 **Integração com Tecnologias Emergentes**

Para maximizar a eficiência e a transparência, o sistema unificado deve ser desenhado para incorporar tecnologias inovadoras.

- **Inteligência Artificial (IA):** O uso de um algoritmo preditivo baseado em machine learning pode ser aplicado para analisar padrões históricos e sazonais de demanda , permitindo prever estoques necessários e otimizar a distribuição antes de uma crise.
- **Blockchain:** Esta tecnologia pode ser utilizada para garantir a rastreabilidade e a imutabilidade do registro de cada bolsa de sangue, desde a coleta até a transfusão, aumentando a transparência e a segurança.
- **Integração com Plataformas Nacionais:** O sistema deve ser capaz de se integrar a iniciativas governamentais, como a Rede Nacional de Dados em Saúde (RNDS), que busca unificar dados de saúde no Brasil.

3 **CONCLUSÃO**

Considerando a análise técnica e estratégica conduzida neste Projeto Integrado Multidisciplinar (PIM) III, a conclusão é clara: a **unificação da Rede Nacional de Bancos de Sangue Públicos no Brasil** não é apenas uma melhoria operacional, mas uma **necessidade urgente de segurança pública e de saúde**. Os objetivos de pesquisar e propor uma arquitetura segura, uma estrutura de banco de dados centralizada, um programa de segurança robusto e demonstrar ganhos de eficiência foram plenamente alcançados.

3.1 **Síntese da Solução e Ganhos de Eficiência**

A solução proposta – uma arquitetura WAN híbrida segura com VPNs criptografadas e um Banco de Dados Relacional Centralizado em Nuvem – resolve a raiz do problema: a fragilidade da descentralização. O impacto da integração pode ser quantificado de forma drástica:

- **Redução do Tempo de Busca:** A eliminação da consulta sequencial a 32 hemocentros resulta em uma busca por bolsas de sangue **32 vezes mais rápida,** o que se traduz em vidas salvas em situações de emergência.
- **Maior Disponibilidade:** A migração para a nuvem aumenta a disponibilidade do sistema de cerca de 72% para 99,99%, garantindo que o sistema esteja acessível mesmo em crises ou desastres.
- **Economia e Logística:** A otimização logística, apoiada em modelagem matemática e na visão nacional de estoque, projeta uma redução de 10% no desperdício de bolsas, gerando uma economia anual de aproximadamente R$ 5 milhões.

3.2 **O Imperativo da Segurança e Ética**

O projeto demonstra que a segurança dos dados e a proteção à vida caminham juntas. O Programa de Segurança da Informação (PSI), baseado em ISO 27001 e LGPD, garante que, ao centralizar os dados, a instituição cumpra seu dever ético. A proteção dos dados sensíveis dos doadores não é um custo, mas um incentivo crucial à doação. A implementação de mecanismos de Gerenciamento de Identidade e Acesso (IAM) e criptografia IPsec se torna o alicerce para manter a confiança do público e a integridade da Hemorrede.

3.3 **Perspectivas Futuras e Integração Tecnológica**

Olhando para frente, a infraestrutura unificada serve como uma plataforma para a inovação. Tecnologias emergentes, como a Inteligência Artificial (IA), podem ser integradas para criar algoritmos preditivos que antecipam demandas sazonais e evitam a escassez. A integração com a RNDS (Rede Nacional de Dados em Saúde) e o eventual uso de Blockchain para rastreabilidade consolidarão o Brasil na vanguarda da gestão de dados em saúde.

Em suma, embora os desafios de implementação (como a resistência cultural e o investimento inicial de R$ 2 milhões) sejam reais, os benefícios sistêmicos, sociais e éticos da unificação superam amplamente os riscos. Este projeto é a base para uma Hemorrede Pública mais eficiente, resiliente e segura, cumprindo a missão fundamental de salvar vidas no país.

REFERÊNCIAS

AGÊNCIA GOV. **Dia Nacional do Doador de Sangue: país conta com 32 hemocentros.**. 2025. Disponível em: https://agenciagov.ebc.com.br/noticias/202411/dia-nacional-do-doador-de-sangue-saude-reforca-a-importancia-da-doacao-regular. Acesso em: 27 set. 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS.. **Informação e documentação Trabalhos acadêmicos Apresentação**. Rio de Janeiro, 2011. Disponível em: . Acesso em: 27 set. 2025.

FIORCRUZ.. **Seminário de Privacidade e Proteção de Dados debate aplicação da LGPD na saúde.**. Disponível em: https://agencia.fiocruz.br/seminario-de-privacida. Acesso em: 27 set. 2025.

GIL, A. C.. **Como elaborar projetos de pesquisa**. São Paulo, 2002. Disponível em: . Acesso em: 27 set. 2025.

GOV.BR. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd. Acesso em: 27 set. 2025.

HEMOCENTROS UNIDOS. **Números de doações de sangue na Hemorrede Pública Brasileira em 2024**. 2025. Disponível em: https://hemocentrosunidos.org.br/noticias/numeros-de-doacoes-de-sangue-na-hemorrede-publica-brasileira-em-2024. Acesso em: 27 set. 2025.

JOTA. **Brasil posiciona-se na vanguarda global da gestão de dados em saúde**. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/coluna-fernando-aibrasil-posiciona-se-na-vanguarda-global-da-gestao-de-dados-em-saude. Acesso em: 27 set. 2025.

MINISTÉRIO DA SAÚDE. **Doação de Sangue**. Disponível em: https://www.gov.br/saude/pt-br/campanhas-da-saude/2025/doacao-de-sangue. Acesso em: 27 set. 2025.

MINISTÉRIO DA SAÚDE. **Ministério da Saúde lança campanha para incentivar doação regular de sangue**. 2025. Disponível em: https://www.gov.br/saude/pt-br/assuntos/noticias/2025/junho/ministerio-da-saude-lanca-campanha-para-incen. Acesso em: 27 set. 2025.

Pearson Prentice Hall. **Redes de computadores**. São Paulo, 2011. Disponível em: . Acesso em: 27 set. 2025.